REMARKS

Claims 1-23 are pending. Claims 1, 4, 9, 14, 15, 18, 20, and 21 have been amended. These amendments are presented in order to more clearly recite features that are already present in the claims and are not intended to, and do not, narrow the scope of the claims in any respect. Reconsideration and allowance of the claims in light of the present remarks is respectfully requested.

Discussion of Claim Rejections under 35 USC § 102

Claims 4-5, 8, 15, 18, 20, and 22 stand rejected under 35 U.S.C. § 102(a), (e) as being anticipated by Robinson et al., U.S. Pat. No. 5,915,022 ("Robinson").

Claim 20

Claim 20 stands rejected under Robinson. Claim 20 recites in part: "wherein the encrypted code attached to the transaction certificate is decrypted by the second party to prove the transaction." The Office Action states that Robinson shows instructing the second party to decrypt the encrypted code of the transaction certificate based on a public key of the first party to generate the decrypted selected elements, at column 5, lines 41-53. The Office Action further states that Robinson teaches that decrypted selected elements can be used by the second party to prove the transaction, at column 2, lines 31-43, at column 6, lines 23-67, and at column 7, lines 1-33.

Applicant submits that Robinson fails to show a system wherein the encrypted code attached to the transaction certificate is decrypted by the second party to prove the transaction as recited in Claim 20. Rather, the passages cited by the Office Action differ from the language of the claims in that they show that a transaction certificate is decrypted by the first party to prove the transaction, not the second party as provided in Claim 20. For example, at column 6, lines 48-53, Robinson states:

> Finally, in step 126, the customer preferably saves the confirmation page along with the encrypted transaction record appended thereto. As will be explained in further detail with respect to Figure 5, if the customer saves the confirmation page, he may later present it to the merchant in the event of a dispute over the transaction.

Thus, the customer in Robinson, e.g., the second party, saves the confirmation page along with the encrypted transaction. The second party does not decrypt the transaction certificate as recited in Claim 20.

Figure 1-2 in Robinson further confirms that it is the first party that decrypts the transaction certificate in order to prove the transaction rather than the second party as is recited in Claim 20. At blocks 124 and 126 in the figure, Robinson shows that a digital receipt page is received by the customer, e.g., the second party, and that the customer saves the digital receipt page. Nowhere in that figure does Robinson teach or suggest that the customer decrypts the encrypted transaction record. Further, at Figure 5, step 140, the customer presents the digital receipt page to the merchant, e.g., the first party. It is the merchant, e.g., the first party, who decrypts the transaction record at step 144 in Figure 5, not the customer.

Claim 15

The Office Action also rejects Claim 15 as being anticipated by Robinson. Amended Claim 15 recites in part "decrypting by the second party the included encrypted code based on the retrieved public key of the first party to generate decrypted proof elements, wherein the decrypted proof elements are used to prove the transaction." The Office Action states that, at column 5, lines 47-50, Robinson teaches that a customer could obtain the merchant's public key and could be able to decrypt the transaction receipt. The Office Action further states that, at column 2, lines 31-43, column 6, lines 23-67, and column 7, lines 1-33, Robinson shows that decrypted proof elements are used to prove the transaction.

Applicant submits that Robinson fails to teach or otherwise disclose a system for decrypting "encrypted code based on the retrieved public key of the first party to generate decrypted proof elements, wherein the decrypted proof elements are used to prove the transaction." The Office Action relies on Robinson's statement that a customer could hypothetically obtain the merchant's public key and could decrypt the transaction receipt. However, Robinson does not go on to provide any description of how a customer, having obtained the merchant's public key and decrypted the transaction receipt to generate proof elements, could then use that those proof elements generated from the decrypted receipt to prove the transaction. Rather, any use of decrypted proof elements to prove the transaction in Robinson occurs only after the vendor decrypts the proof elements using its own private key. Thus,

Robinson fails to teach at least these features, and Claim 15 is therefore allowable over Robinson.

Claim 4

Claim 4 recites in part "instructing the second party to decrypt the encrypted code of the transaction certificate based on a public key of the first party to generate decrypted selected elements . . .." This feature is similar to those found in Claims 20 and 15 as discussed above. Accordingly, Claim 4 is additionally allowable for substantially similar reasons. In addition, Applicant submits that Robinson does not anticipate Claim 4 because it does not disclose at least "instructing the second party" as recited in the claim. The Office Action states that this feature is shown at "column 5, lines 41-53, customer obtains merchant public key can decrypt the transaction receipt." Office Action at page 3.

At column 5, lines 41-53, Robinson states:

> In the case where a public key cryptosystem is used in step 115, it is preferred that the merchant use its own secret key so that no other party may re-encrypt an altered version of the transaction record. If the merchant's own secret key is used to encrypt the transaction record in step 115, then the merchant need not keep the corresponding public key private. If a customer obtains the merchant's public key, for example, the customer could decrypt the transaction receipt, but would still be unable to re-encrypt an altered version of the receipt without the merchant's secret key. Alternatively, the merchant could use its public key for encryption in step 115, so long as the public key is not distributed.

Nowhere in this cited passage does Robinson indicate that the second party is instructed to decrypt the encrypted code of the transaction certificate as is recited in Claim 4. The passage poses a hypothetical situation in which a customer might obtain a public key and decrypt a transaction receipt, but the reference discloses no instruction to do so.

Claim 18

The Office Action also rejects Claim 18 as being anticipated by Robinson. Claim 18, as amended, recites in part:

> A method of a third party authenticating a transaction conducted between a first party and a second party, the method comprising:
>
> retrieving, by a third party, a transaction certificate with an encrypted code;
>
> . . .

> decrypting the encrypted code based on the retrieved public key of the first party to generate decrypted proof elements . . . .

The Office Action states that Robinson teaches a method of a third party authenticating a transaction conducted between a first party and a second party. Applicant submits that Claim 18 is allowable for at least two reasons. First, Robinson does not teach or otherwise suggest a third party authenticating a transaction conducted between a first party and a second party as recited in the claim. Only two parties, the merchant and the customer, are described. Moreover, as discussed previously in connection with Claim 20, Robinson shows a system in which the first party, e.g., the merchant, does both the encrypting and the decrypting using its private key. It would make no sense for the merchant in Robinson (the first party) to retrieve its own public key for the purpose of decrypting a document, when it could decrypt the document with a private key that it already possessed. Robinson does not disclose the first party retrieving a public key and then using the public key to generate decrypted proof elements as recited in Claim 18, as it would use its private key to do so instead. Thus, Claim 18 is allowable over Robinson.

Claim 22

Claim 22 also stands rejected as being anticipated by Robinson. Claim 22 recites in part "a first decryption module configured to decrypt the encrypted code to generate decrypted proof elements, based on a public key of the first party, wherein the decrypted proof elements are used to prove the transaction." As was discussed previously in connection with Claim 15, Robinson discloses that a customer hypothetically could obtain a merchant's public key and decrypt the transaction receipt. However, Robinson never discloses that any proof elements generated by the customer using the merchant's public key could be used for proving the transaction. The system contemplated by Robinson only contemplates a customer presenting a still encrypted receipt to a merchant. See Column 8, lines 38-57 ("In step 140, the customer presents a digital receipt page to the merchant computer . . . . In steps 144 and 146, the transaction record is decrypted by the merchant computer and the transaction information is extracted . . . . Since the transaction record was originally encrypted under the direction of the merchant, the merchant computer simply uses the same private key to extract the transaction data.") Thus, Robinson fails to teach or otherwise disclose the claimed feature of a first decryption module configured to "decrypt the encrypted code to generate decrypted proof elements, based upon a public key of the first party," where

those decrypted proof elements are then used to prove the transaction as is recited in Claim 22. Thus, Claim 22 is also allowable over Robinson.

Discussion of Rejections Under 35 U.S.C. § 103(a)

Claims 1-3, 6-7, 11-14, and 17 and rejected under 35 U.S.C. § 103(a) as being unpatentable over Robinson in view of Zhao et al., U.S. Pat. No. 6,243,480 ("Zhao").

Claim 1

The Office Action states that Claim 1 is unpatentable over Robinson in view of Zhao. The Examiner concedes that Robinson does not disclose printing at least a portion of the received transaction elements on a hardcopy transaction certificate, nor does it disclose printing the encrypted code on the hardcopy transaction certificate and instructing the second party to scan the transaction certificate to convert the encrypted code to electronic form. The Office Action relies on Zhao stating that Zhao teaches receiving a hardcopy of a document with partial authentication information and scanning the analog reference to convert the encrypted code into an electronic form for verification, at column 3, line 57 – column 4, line 14. According to the Office Action, it would have been obvious to one of ordinary skill in the art to print out a hardcopy of the transaction receipt to be scanned in at a later time to verify a transaction. As Zhao states, at column 3, lines 41-54, that such a modification would provide a way to authenticate a digital receipt that has been printed out without losing the authentication information.

Claim 1 recites in part "instructing the second party to scan the transaction certificate to convert the encrypted code to electronic form." Applicant submits that Claim 1 is allowable over the combination of Zhao and Robinson, even if proper, for at least the following reasons. First, neither Zhao nor Robinson teaches instructing the second party to do anything. Thus, the combination cannot read on Claim 1. Second, as discussed above in connection with Claims 4, 15 and 22, the passage relied upon by the Examiner to show decrypting encrypted code based on a public key of the first party is merely a hypothetical posed by Robinson and is expressly disclaimed, at column 6, lines 2-5. Moreover, as discussed above, decrypted selected elements in Robinson are used only by the first party (e.g., the merchant) to prove the transaction, not the second party as recited in Claim 1. Accordingly, Claim 1 is allowable.

Claim 14

Claim 14 also stands rejected over the combination of Zhao and Robinson. Applicant submits that, as with allowable Claims 4, 15 and 22, Claim 14 also includes the feature of "decrypting the converted encrypted code based on the retrieved public key of the first party to generate decrypted proof elements, wherein the decrypted proof elements are used to prove the transaction." Applicant submits that the combination of Zhao and Robinson, even if proper, fails at least to teach decrypting the encrypted code based on the retrieved public key of the first party and using it to generate decrypted proof elements wherein those decrypted proof elements are used to prove the transaction. As discussed above in connection with Claim 15, Robinson fails to disclose using decrypted proof elements to prove the transaction because it shows only a system in which the merchant uses its private key to decrypt code and prove the transaction.

Claim 17

Claim 17 also stands rejected under a combination of Robinson and Zhao. The Office Action alleges that Robinson teaches a method of a third party authenticating a transaction conducted between a first party and a second party. Applicant submits that, as was pointed out in connection with Claim 18 above, Robinson provides no disclosure regarding third party authentication at all. For at least this reason, Claim 17 is allowable over Robinson. Moreover, Zhao does not cure this deficiency in Robinson. Therefore, the claim is allowable.

Claims 9, 10, 16, 19, 21, and 23

Claims 9, 10, 16, 19, 21, and 23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Robinson in view of Powar, U.S. Pat. No. 6,285,991 (Powar).

With respect to Claims 9 and 21, the Office Action concedes that Robinson does not disclose retrieving a public key of the second party to generate an encrypted transaction certificate; transmitting the encrypted transaction certificate to the second party; and instructing the second party to decrypt the transmitted encrypted transaction certificate based on a private key of the second party to produce a decrypted transaction certificate that includes the encrypted code. The Office Action instead relies on Powar, stating that Powar teaches sending a statement to a customer using a customer's public key system at column 4, line 55 to column 5, line 17, and at column 11, lines 1-50.

Applicant respectfully submits that the neither Robinson nor Powar, alone or in combination, teaches "instructing the second party to decrypt the transmitted encrypted

transaction certificate" or "instructing the second party to decrypt the included encrypted code" as recited in Claim 9. Neither Robinson nor Powar teaches instructing a second party to do anything. Accordingly, Claim 9 is allowable over the combination of Robinson and Powar.

Regarding Claim 21, Applicant also submits that neither Robinson nor Powar, alone or in combination, disclose a system wherein an encrypted code is decrypted based on a public key of the first party to generate decrypted selected elements proof elements, and using proof elements generated in such a way for proving the transaction. The system contemplated by Robinson only contemplates a second party presenting a still encrypted receipt to a first party, wherein the first party then decrypts the receipt using its private key. See Column 8, lines 38-57 ("In step 140, the customer presents a digital receipt page to the merchant computer . . . . In steps 144 and 146, the transaction record is decrypted by the merchant computer and the transaction information is extracted . . . . Since the transaction record was originally encrypted under the direction of the merchant, the merchant computer simply uses the same private key to extract the transaction data.") Thus, Robinson and Powar fail to teach each element in Claim 21, and Claim 21 is allowable.

Claim 16 also stands rejected under the combination of Robinson and Powar. Claim 16 includes the recited feature of "decrypting the encrypted code based on the retrieved public key of the first party to generate decrypted proof elements, wherein the decrypted proof elements are used to prove the transaction." The Office Action states that Robinson teaches this claimed feature. However, as was discussed above in connection with Claim 15, any use of decrypted proof elements to prove the transaction in Robinson occurs only after the vendor decrypts the proof elements using its own private key. Powar does not cure this deficiency. Accordingly, Claim 16 is allowable.

The Office Action also rejects Claim 19 as being obvious over the combination of Robinson and Powar. Claim 19 recites in part:

> A method of a third party authenticating a transaction conducted between a first party and a second party, the method comprising:
>
> . . .
>
> decrypting the received encrypted transaction certificate based on a private key of the third party so as to generate a transaction certificate with an encrypted code . . . .

The Examiner concedes that Robinson provides no disclosure of decrypting the received transaction certificate based on a private key of the third party so as to generate a transaction certificate with an encrypted code. The Examiner relies on Powar by stating that Powar teaches sending an encrypted statement using a public key system. According to the Office Action, it would have been obvious to one of ordinary skill in the art to encrypt the transaction certificate for transmission to the party.

Applicant submits that even if Powar discloses what is alleged, it makes absolutely no reference to the involvement of a third party (in addition to the first and second party) in the transaction as is recited in the claims. Thus, the cited references fail to teach or otherwise suggest a method of a third party authenticating a transaction as provided in Claim 19. Accordingly, Claim 19 is allowable over the cited references.

Claim 23 also stands rejected under Robinson and Powar. Claim 23 recites in part, "a second decryption module configured to decrypt the encrypted code based on a public key of the first party to generate decrypted proof elements, wherein the decrypted proof elements are used to prove the transaction." The Office Action states that Robinson teaches this feature at column 5, lines 41-53 and at columns 2, 6, and 7. Applicant submits that Robinson never discloses that any proof elements generated by a second decryption module based on a public key could be used for proving the transaction. The system contemplated by Robinson only contemplates a customer presenting a still encrypted receipt to a merchant. See Column 8, lines 38-57 ("In step 140, the customer presents a digital receipt page to the merchant computer . . . . In steps 144 and 146, the transaction record is decrypted by the merchant computer and the transaction information is extracted . . . . Since the transaction record was originally encrypted under the direction of the merchant, the merchant computer simply uses the same private key to extract the transaction data.") Thus, Robinson fails to teach or otherwise disclose the claimed feature of a second decryption module configured to "decrypt the encrypted code to generate decrypted proof elements, based upon a public key of the first party," where those decrypted proof elements are then used to prove the transaction as is recited in Claim 23. Powar does not cure this deficiency. Thus, Claim 23 is allowable.

Dependent Claims

Claims 2-3, 5-8 and 10-13 are dependent either directly or indirectly on the discussed independent claims. Applicant respectfully submits that pursuant

¶4, the dependent claims incorporate by reference all the limitations of the claim to which they refer and include their own patentable features, and are therefore in condition for allowance. Therefore, Applicant respectfully requests the withdrawal of all claim rejections and prompt allowance of the claims.

CONCLUSION

In light of the above, reconsideration and withdrawal of the outstanding rejections are specifically requested. In view of the foregoing remarks, Applicant respectfully submits that the claims of the above-identified application are in condition for allowance. However, if the Examiner finds any impediment to allowing all claims that can be resolved by telephone, the Examiner is respectfully requested to call the undersigned.

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 12/28/05

By: _____

John M. Carson
Registration No. 34,303
Attorney of Record
Customer No. 20,995
(619) 235-8550

2245344_1
122805